




JOHN NAIMO
AUDITOR-CONTROLLER

COUNTY OF LOS ANGELES DEPARTMENT OF AUDITOR-CONTROLLER

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-3873
PHONE: (213) 974-8301 FAX: (213) 626-5427

May 18, 2016

TO: Supervisor Hilda L. Solis, Chair
Supervisor Mark Ridley-Thomas
Supervisor Sheila Kuehl
Supervisor Don Knabe
Supervisor Michael D. Antonovich

FROM: John Naimo 
Auditor-Controller

SUBJECT: **FEASIBILITY OF CONDUCTING ANNUAL INFORMATION
TECHNOLOGY AND SECURITY POLICY AUDITS (Board Agenda July
14, 2015, Item 8)**

On July 14, 2015, the Board of Supervisors (Board) approved a motion directing the Auditor-Controller (A-C), in coordination with the Interim Chief Executive Officer (CEO), to report back in 60 days on the feasibility of conducting Information Technology (IT) and Security Policy Reviews of every County department, including the CEO and Executive Office of the Board, on an annual basis.

On November 16, 2015, the CEO, in coordination with the A-C, reported to the Board five scenarios that estimated the cost of performing IT and Security Policy Reviews based on varying frequencies. However, the A-C and CEO estimated the costs to be significant and determined that the A-C would expand its current IT risk assessment before recommending any of the scenarios or other alternatives. To expand the risk assessment, the CEO notified the Board that \$300,000 was available to contract with an outside IT security vendor to conduct a limited assessment of IT risk vulnerabilities and policies, and incorporate the results of the assessment into the A-C's current risk assessment.

Current Status

After careful evaluation of recent IT audit findings and our IT audit operations, we determined that the IT security vulnerabilities and internal control weaknesses identified within our reports are generally the result of non-compliance with established County IT standards defined within the Board Policy Manual and County Fiscal Manual (CFM). These same findings are not a result of emerging IT risks currently not known to

departments or captured in the A-C's IT risk assessment. As a result, contracting for limited IT assessments in an effort to expand our current IT risk assessment, as previously suggested by the CEO, would probably not result in significant changes to our assessment or the IT audits we perform.

We believe that our current audit focus on higher risk IT control areas, plus a variety of proposed new initiatives to annually review and report on targeted high-risk control areas Countywide, will address the Board's IT security concerns. Our audits and the new initiatives will provide IT security assurance services that are significantly less costly than annual IT and Security Policy Reviews of all County departments.

Current staffing and IT audit efforts, and the proposed new Countywide IT audit initiatives, are discussed below.

Current A-C IT Audit Function

The A-C's IT audit function currently consists of eight positions at an annual cost of approximately \$1,200,000. IT audit planning is significantly influenced by our annual Countywide assessment of departments' relative IT risks. The assessment considers risk attributes such as the size and complexity of each department's IT systems and operations, the type and sensitivity of data maintained (e.g., Protected Health Information, financial records, etc.), and the numbers of mission-critical systems, users, computing devices, transactions, and associated dollar values.

In general, the IT audit team performs five major types of assignments to address the various high-risk IT areas. The assignments include reviews of:

- Departments' overall IT operations for compliance with Board IT Policy requirements.
- Departments' controls over high-risk, individual mission-critical systems to evaluate transaction processing, access, and overall system administration.
- electronic Countywide Accounting and Purchasing System (eCAPS) enterprise system and central operations/controls within the A-C to evaluate Countywide compliance with CFM requirements.
- Departments' requests to automatically issue payments processed within their departmental systems and interfaced through eCAPS.
- Departments' requests for eCAPS access that deviate from CFM requirements.

Attached are additional details on the range of assignments that we perform.

Proposed New Countywide IT Security Audit Initiatives

To enhance our current efforts, we are also pursuing various new Countywide IT security audit initiatives that will broaden our audit coverage and report to the Board on

the County's compliance posture in select IT control areas. The following are some examples of these initiatives:

- **Annual Countywide Reviews of Terminated Employees with Access to County Systems.**
 - **Review of eCAPS and electronic Human Resources (eHR) System Enterprise Systems Access** – Our most recent review in this area (mentioned above) disclosed that departments need to be more vigilant in removing eCAPS/eHR access for employees who leave County service. We believe conducting this review annually will help continually improve departments' compliance.
 - **Review of Multiple Departments' Non-Enterprise Systems Access** – Review of user access management across a sampling of multiple departmental systems to determine whether departments remove systems access for employees who leave County service.
- **Annual Countywide Reviews of IT Equipment Management** – Review of IT equipment management across a sampling of multiple County departments to determine whether department's maintain accurate IT equipment inventories and proper accountability of their IT equipment. Prior reviews at individual departments identified misplaced desktops and laptops that may have contained sensitive information (e.g., social security numbers, medical records, etc.).
- **Annual Countywide Reviews of IT Device Encryption and Antivirus** – Review of desktop and laptop encryption and antivirus across a sampling of multiple County departments to determine whether departments have implemented an encryption and antivirus solution on their devices to protect County data.
- **Annual Countywide Reviews of Internet Protocol (IP) Address Management** – Review of IP address management at the Internal Services Department (ISD) and across a sampling of multiple County departments to determine whether policies and procedures help ensure County network communications (wired and wireless) can be tracked to authorized users, and that the users understand their responsibilities for complying with acceptable use rules in the Board IT Policy 6.105 Internet Use Content.
- **Annual Self-Certification Reporting** – Annual review of each department's compliance with critical IT control areas as self-certified in the Internal Control Certification Program (ICCP). The A-C is enhancing the current ICCP process to improve focus on critical controls, and we will conduct spot checks of departments' reported compliance in critical areas of particular interest to the Board.

Other IT Security Audit Initiatives/Efficiencies

There are many Countywide IT security programs/initiatives that are critical to the County's overall IT security strategy, which are the responsibility of central departments such as ISD and CEO. In our ongoing effort to increase the efficiency and effectiveness of our audits, we plan to evaluate performing audits of these central departments' Countywide administration of areas such as network vulnerability, network threat prevention/detection, IT asset management, IT security training, and other centralized IT control areas. In addition, we will evaluate acquiring software/tools, such as network vulnerability scanning software, to assist in performing the audits/assignments discussed throughout this report.

A-C Proposal

IT system management and data security should be top priorities in the County. We believe that the A-C's historical focus on high-risk IT control areas, plus the new Countywide initiatives described above, provide a more reasonable, effective, and significantly less costly approach to IT security than annual IT and Security Policy Reviews of all County departments.

We also believe our current comprehensive IT audit risk assessment will help target high-risk IT areas in the County, and that contracting for limited IT assessments, as previously directed, would not result in significant changes to our risk assessment or the IT audits/assignments we perform.

Unless otherwise directed, we will continue with our existing IT audit coverage while pursuing a variety of new initiatives and efficiencies as described above. We are working with the CEO on funding for the new initiatives and software/tools as part of the Fiscal Year 2016-17 budget process.

If you have any questions please call me, or your staff may contact Robert Smythe at (213) 253-0100.

JN:AB:PH:RS:MP

Attachment

c: Sachi A. Hamai, Chief Executive Officer
Jim Jones, Chief Operating Officer, Chief Executive Office
Lori Glasgow, Executive Officer, Board of Supervisors
Dave Chittenden, Chief Deputy Director, Internal Services Department
Public Information Office
Audit Committee

CURRENT AUDITOR-CONTROLLER INFORMATION TECHNOLOGY AUDIT ASSIGNMENTS

The Auditor-Controller (A-C) Information Technology (IT) audit team performs five major types of assignments to address the various high-risk IT areas. The following describes the range of assignments we perform:

- **Departmental IT and Security Policy Reviews** – Comprehensive reviews of County departments' overall IT operations for compliance with Board IT Policy requirements, such as antivirus, encryption, security training, facility security requirements, and computing device inventory controls. The reviews include samplings of the audited departments' multiple systems and computing devices. The recent IT audits of the Departments of Public Health and Probation are examples of these types of reviews.
- **Individual Mission-critical System Reviews** – Reviews of controls and related processes over high-risk, individual mission-critical systems. These reviews evaluate the accuracy and validity of transaction processing, the appropriateness of access assignments, including privileged access to critical County data (e.g., financial data, health records, etc.), and the administration over individual systems to ensure compliance with County Fiscal Manual (CFM) requirements.

These reviews have identified transaction inaccuracies/improprieties resulting in overpayments and under-billings, transaction processing delays that resulted in penalties and interest charges to the County, and inappropriate access controls, including the sharing of user identification and passwords which increase the risk for inappropriate activity. Examples of System Reviews that we have conducted include the Assessor's Secured Property Systems, Sheriff's Garnishment System (MAPAS), the Department of Health Services' Community Health Plan Patient Management System, and the County's Risk Management and Claims Administration Information System.

- **electronic Countywide Accounting and Purchasing System (eCAPS) Enterprise System and Central Operations/Controls Reviews** – Countywide reviews of eCAPS and electronic Human Resources (eHR) System users and transactions for compliance with CFM requirements, and reviews of central eCAPS operations/controls within the A-C. eCAPS and eHR are the County's enterprise financial and human resources systems, each with thousands of users responsible for processing annual payments and payroll transactions totaling over \$15 billion and \$7 billion, respectively.

The reviews help determine compliance with certain IT control requirements designed to prevent unauthorized access, inappropriate activity, etc., and to determine the adequacy of central controls. Our recent review of Terminated Employees with eCAPS and/or eHR Access is an example of this type of review.

Our IT audit function will continue to evaluate ways to perform similar Countywide reviews of other central controls/operations.

- **eCAPS Interface Reviews** – Reviews of departments' requests to automatically issue payments processed within their departmental systems and interfaced through eCAPS. Although not audits, the reviews evaluate departments' reported controls and procedures over the electronic interface process prior to authorizing the interface to occur. This helps ensure that the interfaces, many of which process millions of dollars in payments annually, have proper controls in place and are in compliance with County rules prior to implementation.

We have reviewed numerous interface processes, including the interfaces for the Department of Children and Family Services' Approved Relative Caregivers/Automated Provider Payment System, Superior Court's Jury Management Information System, and the Department of Public Social Services' Generic Contract Invoicing System.

- **eCAPS Access Exceptions** – Evaluation of departments' requests for eCAPS access that deviate from CFM requirements. The reviews evaluate internal control deficiencies and help establish compensating controls/processes in critical operations that must be implemented before the exception requests are granted.